Integrated Sensing and Processing (ISP) Phase II: Demonstration and Evaluation for Distributed Sensor Networks and Missile Seeker Systems

Progress Report:

Waveform Design Technical Template

17 November 2005

Acknowledgment of Support
This material is based upon work supported by the United States Air Force under Contract No. N00014-04-C-0437.

Contract No.: N00014-04-C-0437
Contract Line Item Number 0001
Deliverable Item: Publications (A002-001)

Raytheon Company
P.O. Box 11337
Tucson, AZ 85734-1337

Distribution Statement A.

Approved for public release.
Distribution is unlimited.

DESTRUCTION NOTICE

For classified documents, follow the procedures in DOD 5220.22M, National Industrial Security Program Operating Manual (NISPOM), Chapter 5, Section 7, or DOD 5200.1-R, Information Security Program Regulation, Chapter IX. For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **17 NOV 2005**	2. REPORT TYPE	3. DATES COVERED

4. TITLE AND SUBTITLE **Integrated Sensing and Processing Phase II: Waveform Design Template**	5a. CONTRACT NUMBER **N00014-04-C-0437**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Raytheon Missile System,1151 Herman Rd ,Tucson,AZ,85706**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

We introduce a new mathematical design methodology for families of codes, suitable for different applications in Radar and Communications. The techniques are derived from Mulitiresolution Harmonic Analysis as well as a general result of Benke [2], regarding Rudin- Shapiro Polynomials. Some explicit estimates for the performance of the algorithms are also given.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**1**	**22**	

Integrated Sensing and Processing Phase II: Technical Report

Part Two

Construction of Coded Waveforms: Benke Approximation Schemes for High-performance Code Design

Paolo Emilio Barbano & Ronald R. Coifman
Yale University

Harry Schmitt
Raytheon Company

November 17, 2005

Abstract

We introduce a new mathematical design methodology for families of codes, suitable for different applications in Radar and Communications. The techniques are derived from Mulitiresolution Harmonic Analysis as well as a general result of Benke [2], regarding Rudin-Shapiro Polynomials. Some explicit estimates for the performance of the algorithms are also given.

Motivation and Background

Since the classic work of Golomb [5], numerous mathematical techniques have been devoleped for the generation of code families with high auto- and cross-correlation performance. With few exceptions though (e.g. [3], [1]), researchers in the field have been interested in the developement of the algebraic aspect of the theory of code design. The goal of the present paper is to demostrate how analytical techniques can provide higher flexibility to build different requirements into the algorithms. In order to achive this, we propose here some techniques which make extensive use of tools from Mulitiresolution Harmonic Analysis as well as a general result of Benke ([2]) regarding the fundamental construction of Rudin-Shapiro Polynomials. More specifically, we consider codes and code-families as finite approximants of bases in infinite-dimentional function spaces (e.g. $L^2([0,1])$ and $L^2(\mathbb{R})$). An approximation scheme is exhibited with the desired asymptotic properties. We then obtain a variety of new code generation algorithms and provide some explicit estimates for their performance.
The paper is therefore naturally divided in three parts: a first part, containing a short review of relevant results, the second, providing statements and proofs of the main theorems, and a third one, with numerical results a short discussion of future work.

1 Algebraic and Anlaytic Code Design

To motivate our approach to the design problem of coding sequences, we will follow the historical development of the subject through the theory of *Shift Register Sequences*. Solomon Golomb's classic text was our guide in this [5]. Let's begin with some preliminaries.

1.1 Shift Register Sequences

Linear shift registers are very important for the *algebraic* theory of error-correcting codes. In a shift register (SR), eventually, a sequence will repeat. This is because for a binary SR sequence, there are only 2^r possible states (either on or off, for each tube). So, a repetition occurs in the first 2^r states. However, we can improve on that bound, since if we have a state of all 0's, the shift register will continue producing 0's, which means its period is just 1. So, the period of a binary shift register is at most $2^r - 1$.

Definition A sequence generated by an r-tube shift register will be said to have *maximum length* if its period is $p = 2^r - 1$.

Lemma 1.1 *Any r inputs and r outputs of a maximum length r-tube shift register sequence completely determine all of the outputs.*

Proof Consider r inputs $\{a_1, a_2, \ldots, a_r\}$ and r outputs $\{b_1, b_2, \ldots, b_r\}$.
Then,

$$\begin{aligned} b_1 &\equiv c_1 a_r \oplus c_2 a_{r-1} \oplus \cdots \oplus c_r a_1 \quad (mod 2) \\ b_2 &\equiv c_1 b_1 \oplus c_2 a_r \oplus \cdots \oplus c_r a_2 \quad (mod 2) \\ &\vdots \\ b_r &\equiv c_1 b_{r-1} \oplus c_2 b_{r-2} \oplus \cdots \oplus c_r a_r \quad (mod 2) \end{aligned}$$

So, we want to find the recursion coefficients, $\{c_1, c_2, \ldots, c_r\}$. Hence, in matrix form this system becomes:

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \end{pmatrix} = \begin{pmatrix} a_r & a_{r-1} & \cdots & a_1 \\ b_1 & a_r & \cdots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ b_{r-1} & b_{r-2} & \cdots & a_r \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_r \end{pmatrix}$$

Hence,

$$\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_r \end{pmatrix} = \begin{pmatrix} a_r & a_{r-1} & \cdots & a_1 \\ b_1 & a_r & \cdots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ b_{r-1} & b_{r-2} & \cdots & a_r \end{pmatrix}^{-1} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \end{pmatrix}$$

if the inverse exists.

Assume that it does not. Then, there is a row such that it is a $\mathbb{Z}_2$ multiple of another row. Hence, it is either equal to that row or is a row of 0's.
Say it is the latter. So, say the k-th row is all 0's. If $k \neq 1$, then

$$b_1 = \cdots = b_{k-1} = b_k = a_r = \cdots = a_k = 0.$$

But, this means that

$$b_{k+1} = c_1 b_k \oplus \cdots \oplus c_k b_1 \oplus c_{k+1} a_r \oplus \cdots \oplus c_r a_{k+1} = 0c_1 \oplus \cdots \oplus 0c_r = 0.$$

In the same manner, we see that all the b_k are 0, meaning that we have a blank tape, contradicting that the shift register has maximum length. If $k = 1$, then all the a_i are 0, meaning that all the inputs are 0. This implies that all the outputs are 0, which is again a contradiction.

Now, say that there is a row equal to another row. Let the j-th row equal the $k+j$-th row. Then, it can be seen that the elements of the sequence: $\{a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_r\}$ repeat every k elements. Hence, the sequence has period k, contradicting that it is of maximum length, since $k < r < 2^r - 1$.

So, the matrix is invertible. Hence, we can solve for $c_1, \ldots, c_r$. Now, construct the matrix:

$$C = \begin{pmatrix} c_1 & 1 & 0 & \cdots & 0 \\ c_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_r & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Then,

$$\begin{pmatrix} a_n a_{n+1} \cdots a_{n+r} \end{pmatrix} \begin{pmatrix} c_1 & 1 & 0 & \cdots & 0 \\ c_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_r & 0 & 0 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} a_{n+r+1} a_{n+r+2} \cdots a_{n+2r} \end{pmatrix}$$

for all n. Hence, this matrix yields the entire output. ▌

Remark To see that the general case (for $\mathbb{Z}_p$) is also true, we use the same argument, only this time, we assume that some row is a $\mathbb{Z}_p$ multiple of another. So, say that $\vec{v}_j$ is the j-th and $\vec{v}_{k+j}$ is the $k+j$-th row. Then, $\vec{v}_j \equiv d\vec{v}_{k+j} \pmod{p}$. So, we see that after every k outputs, the next k outputs are d times the previous set of k outputs. Now, by Fermat's Little Theorem, $d^{p-1} \equiv 1 \pmod{p}$. This means that after $k(p-1)$ places, the sequence repeats. But, $k(p-1) < p^r - 1$. Hence, the sequence is not of maximum length. This is a contradiction. Hence, the rows are linearly independent and the rest of the argument from above follows.

In a variety of engineering applications, there arises a need to have "random" sequences. Since a computer is a finite state machine, true randomness can not be produced on it. Hence, there is a need to produce sequences that appear random. A good model for binary random sequences, is flipping a fair coin. From statistics, there are certain things one would expect from such a model:

- The number of $+1$'s (heads) is about the same as the number of -1's (tails).
- Short runs (consecutive streaks of heads or tails) are more likely to occur than long runs. Precisely, half the runs have length 1, one fourth have length 2, one eighth have length 3, etc.
- There is also a certain property about the autocorrelation of such sequences. Autocorrelation measures how similar a sequence is to a shift of itself. One would expect that the autocorrelation peaks at no shift (being identical to itself), and is smaller for positive shifts.

The algebraic definition of a random sequence, which in engineering is called *noise*, is then:

Definition We say that a binary shift register sequence, $A = \{a_1, a_2, \ldots\}$ of period p is a *pseudo-noise sequence* if:

1. $$|\sum_{n=1}^{p} a_n| \leq 1$$
2. For every run of length k, there are two runs of length $k-1$
3. The cyclic autocorrelation function α has the property:
$$p\alpha(A)(\tau) = \sum_{n=1}^{p} a_n a_{n+\tau} = \begin{cases} p & \text{if } \tau = 0 \\ \Omega & \text{if } 0 < \tau < p \end{cases}$$

The three randomness postulates all reflect the model of randomness described above. The third postulate says that the cyclic autocorrelation function is two valued. This comes from the fact that all shift register sequences are periodic. It turns out that all maximum-length shift registers satisfy the three postulates. The proof of this fact is not hard, but is beyond the scope of the present discussion and may be found in Golomb's text.

2 Crosscorrelation and Autocorrelation Properties

After the introductory study of SR sequences, we proceeded to look at Dilip Sarwate's 1979 paper Crosscorrelation and Autocorrelation of Sequences [6]. This provides a good feel for some basic analytical aspects of the project.

Let X be a family of K complex sequences of period N. For sequences, $u, v \in X$, the periodic crosscorrelation function $\gamma(u, v)(\cdot)$ is defined as:

$$\gamma(u, v)(l) = \sum_{i=0}^{N-1} u_i \overline{v_{i+l}}$$

and the periodic autocorrelation function $\alpha(u)(\cdot)$ is defined as:

$$\alpha(u)(l) = \sum_{i=0}^{N-1} u_i \overline{u_{i+l}}$$

We now prove a technical lemma:

Lemma 2.1 *Let u, v be two complex sequences of length N. Then,*

$$\sum_{l=0}^{N-1} |\gamma(u, v)(l)|^2 = \sum_{l=0}^{N-1} \alpha(u)(l)\overline{\alpha(v)(l)}$$

Proof

$$\begin{aligned}
\sum_{l=0}^{N-1} |\gamma(u,v)(l)|^2 &= \sum_{l=0}^{N-1} \gamma(u,v)(l)\overline{\gamma(u,v)(l)} \\
&= \sum_{l=0}^{N-1} \left(\left(\sum_{i=0}^{N-1} u_i \overline{v_{i+l}} \right) \overline{\left(\sum_{j=0}^{N-1} u_j \overline{v_{j+l}} \right)} \right) \\
&= \sum_{l=0}^{N-1} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} u_i \overline{v_{i+l} u_j} v_{j+l} \\
&= \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \sum_{l=0}^{N-1} u_i \overline{v_{i+l} u_j} v_{j+l} \\
&= \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} u_i \overline{u_j} \sum_{l=0}^{N-1} \overline{v_{i+l}} v_{j+l}
\end{aligned}$$

Since the sequences are periodic with period N, we can work modulo N. So, letting $m = j - i$ and $k = i + l$, we notice that:

$$\begin{aligned}
\sum_{l=0}^{N-1} |\gamma(u,v)(l)|^2 &= \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} u_i \overline{u_j} \sum_{l=0}^{N-1} \overline{v_{i+l}} v_{j+l} \\
&= \sum_{i=0}^{N-1} \sum_{m=0}^{N-1} u_i \overline{u_{i+m}} \sum_{k=0}^{N-1} \overline{v_k} v_{k+m} \\
&= \sum_{m=0}^{N-1} \left(\left(\sum_{i=0}^{N-1} u_i \overline{u_{i+m}} \right) \overline{\left(\sum_{k=0}^{N-1} v_k \overline{v_{k+m}} \right)} \right) \\
&= \sum_{m=0}^{N-1} \alpha(u)(m)\overline{\alpha(v)(m)}. \quad \blacksquare
\end{aligned}$$

We are now ready to state the main result of Sarwate's paper. Define the following two numbers A and Γ:

$$\begin{aligned}
\Gamma &= \max\{|\gamma(u,v)(l)| : u, v \in X,\ u \neq v,\ 0 \leq l \leq N-1\} \\
A &= \max\{|\alpha(u)(l)| : u \in X,\ 0 < l \leq N-1\}
\end{aligned}$$

Theorem 2.2 (Sarwate, 1979) *For any set X of K sequences satisfying $\alpha(u)(0) = N$ for all $u \in X$, the following holds:*

$$\left(\frac{\Gamma^2}{N}\right) + \frac{N-1}{N(K-1)}\left(\frac{A^2}{N}\right) \geq 1.$$

Proof For all $u, v \in X$,

$$\sum_{u\in X}\sum_{\substack{v\in X\\u\neq v}}\sum_{l=0}^{N-1}|\gamma(u,v)(l)|^2 + \sum_{u\in X}\sum_{l=0}^{N-1}|\alpha(u)(l)|^2$$

$$\begin{aligned}
&= \sum_{u\in X}\sum_{v\in X}\sum_{l=0}^{N-1}|\gamma(u,v)(l)|^2 \\
&= \sum_{u\in X}\sum_{v\in X}\sum_{l=0}^{N-1}\alpha(u)(l)\overline{\alpha(v)(l)} \quad \text{(by Lemma 2.1)} \\
&= \sum_{l=0}^{N-1}\left(\left(\sum_{u\in X}\alpha(u)(l)\right)\overline{\left(\sum_{v\in X}\alpha(v)(l)\right)}\right) \\
&= \sum_{l=0}^{N-1}|\sum_{u\in X}\alpha(u)(l)|^2 \\
&= \left(\sum_{u\in X}\alpha(u)(0)\right)^2 + \sum_{l=1}^{N-1}|\sum_{u\in X}\alpha(u)(l)|^2 \\
&= K^2N^2 + \sum_{l=1}^{N-1}|\sum_{u\in X}\alpha(u)(l)|^2
\end{aligned}$$

since there are K elements in X and for each, $\alpha(u)(0) = N$ by assumption. Now, for the first term on the left hand side, there are $K(K-1)$ different pairs of sequences in X. For the second term, for $l = 0$, there are K sequences, with $\alpha(u)(0) = N$ for each $u \in X$. Hence, the LHS is bounded from above by $K(K-1)N\Gamma^2 + KN^2 + K(N-1)A^2$. On the other hand, the right hand side is bounded from below by K^2N^2 since the second term is always positive. Hence,

$$\begin{aligned} K(K-1)N\Gamma^2 + KN^2 + K(N-1)A^2 &\geq K^2N^2 \\ \Longrightarrow K(K-1)N\Gamma^2 + K(N-1)A^2 &\geq KN^2(K-1) \\ \Longrightarrow \left(\frac{\Gamma^2}{N}\right) + \frac{(N-1)}{N(K-1)}\left(\frac{A^2}{N}\right) &\geq 1. \quad \blacksquare \end{aligned}$$

Definition We say that a *code* is a complex sequence where each element has norm 1.

Example Consider the family of codes of prime length L: $\mathcal{U} = \{u^{(1)}, u^{(2)}, \ldots\}$, where for all N, $u^{(N)} = \{e^{\frac{2\pi ikN}{L}}\}_{k=0}^{L-1}$. So, let's calculate the constants Γ and A.

$$\begin{aligned} \alpha(u^{(N)})(l) &= \sum_{k=0}^{L-1} e^{\frac{2\pi ikN}{L}} \overline{e^{\frac{2\pi i(k+l)N}{L}}} \\ &= \sum_{k=0}^{L-1} e^{\frac{2\pi ikN}{L}} e^{-\frac{2\pi i(k+l)N}{L}} \\ &= \sum_{k=0}^{L-1} e^{-\frac{2\pi ilN}{L}} \\ &= Le^{-\frac{2\pi ilN}{L}} \end{aligned}$$

Hence, $A = L$. As for Γ,

$$\begin{aligned} \gamma(u^{(N)}, u^{(M)})(l) &= \sum_{k=0}^{L-1} e^{\frac{2\pi ikN}{L}} \overline{e^{\frac{2\pi i(k+l)M}{L}}} \\ &= \sum_{k=0}^{L-1} e^{\frac{2\pi ikN}{L}} e^{-\frac{2\pi i(k+l)M}{L}} \\ &= \sum_{k=0}^{L-1} e^{\frac{2\pi i(kN-kM-lM)}{L}} \end{aligned}$$

Since the codes are periodic with prime period L, we can work Modulo L. Hence, as we vary k, $kN - kM - lM$ eventually cycles through all of $\mathbb{Z}_L$. Then, this sum is just the sum of the L^{th} roots of unity. Hence, they satisfy the equation $\omega^L = 1$. From basic algebra, this sum is $-\frac{a_{L-1}}{a_L}$, where a_{L-1} and a_L are the coefficients of the $(L-1)^{\text{th}}$ and L^{th} terms of the polynomial. Therefore, $\sum_{k=0}^{L-1} e^{\frac{2\pi i(kN-kM-lM)}{L}} = 0$. Hence, $\Gamma = 0$.

Lemma 2.3 *Let X be a family of K codes of period N, as in Theorem 2.4, s.t. $A = N$ and $\Gamma = 0$. Then, $K \leq N$*

Proof Let $A = N, \Gamma = 0$. Then, by Sarwate's Theorem, $\frac{N-1}{K-1} \geq 1$. Hence, $N \geq K$. ▮

Lemma 2.4 *If a family of K codes, X, has the property that $\Gamma = 0$, then, there exists a code u, such that $\alpha(u)(l) = N$ for some $l, 0 < l \leq L-1$.*

Proof By Sarwate's Theorem, if $\Gamma = 0$, $A^2 \geq \frac{N^2(N-1)}{K-1}$ Now, if we represent our codes as vectors $\vec{v}_j$, then we note that if $\Gamma = 0$, for any u_j, u_k $(j \neq k)$, $\langle u_j \; , \; u_k \rangle = 0$. Hence, all of the vectors are linearly independent. Therefore, $K \leq N$. Thus, we see that $A^2 \geq N^2$. Hence, $A \geq N$. But, we also know that $A \leq N$ since the maximum autocorrelation occurs at zero-shift. Therefore, $A = N$. Thus, $\exists u \in X, l > 0,$ s.t. $\alpha(u)(l) = N$. ▮

3 Fourier Transforms

Fourier Transforms serve an important role in signal processing. A code can be considered as a discretely sampled version of a signal of constant amplitude. So, we can extend the use of Fourier Transforms to codes. So, for discrete codes, we will make use of Discrete Fourier Transforms:

Definition Consider a complex periodic code of period N: $\{x_0, x_1, \ldots, x_{N-1}\}$. We define the *Discrete Fourier Transform* as the complex periodic code of period N: $\{\chi_0, \chi_1, \ldots, \chi_{N-1}\}$, where for each $n = 0, 1, \ldots N-1$,

$$\chi_n = \frac{1}{N} \sum_{k=0}^{N-1} x_k e^{\frac{-2\pi i k n}{N}}.$$

Proposition 3.1 *Let $C = \{c_0, c_1, \ldots, c_{N-1}\}$ be a complex periodic code of prime length N. Let $\hat{C} = \{\hat{c}_0, \hat{c}_1, \ldots, \hat{c}_{N-1}\}$ be the DFT of the code. Then,*

$$\alpha(\hat{C})(l) = 0$$

for all $l = 1, \ldots, N-1$.

Proof For each $n = 0, 1, \ldots, N-1$, $\hat{c}_n = \frac{1}{N}\sum_{k=0}^{N-1} c_k e^{\frac{-2\pi ikn}{N}}$. Hence,

$$\begin{aligned}
\alpha(\hat{C})(l) &= \sum_{m=0}^{N-1} \hat{c}_m \overline{\hat{c}_{m+l}} \\
&= \frac{1}{N^2}\sum_{m=0}^{N-1}\left(\left(\sum_{k=0}^{N-1} c_k e^{\frac{-2\pi ikm}{N}}\right)\left(\overline{\sum_{j=0}^{N-1} c_j e^{\frac{-2\pi ij(m+l)}{N}}}\right)\right) \\
&= \frac{1}{N^2}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} c_k e^{\frac{-2\pi ikm}{N}} \overline{c_j e^{\frac{-2\pi ij(m+l)}{N}}} \\
&= \frac{1}{N^2}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1} c_k \overline{c_j} \sum_{m=0}^{N-1} e^{\frac{2\pi i(jm+jl-km)}{N}}
\end{aligned}$$

Note that for each j, k the third summation is just the sum of the N^{th} roots of unity as before since N is prime. Hence, it is 0. Therefore, $\alpha(\hat{C})(l) = 0$. ▮

We can extend the theory of discrete codes to the theory of continuous ones (ie: $L^2(\mathbb{R})$, C^p, etc.). Here, we will make use of the continuous version of the Fourier Transform extensively. Hence, we proceed to extend the discrete results from Section 2 to continuous analogues.

The identity in Lemma 2.1 is true in the discrete case. But what happens in the *continuous* case? We have a natural way of defining crosscorrelations and autocorrelations for continuous signals (or functions), namely via the convolution product. So, if $f, g \in L^2(\mathbb{R})$, we define the crosscorrelation of two functions as:

$$(f \star g)(y) = (f * \overline{\tilde{g}})(y) = \int_{-\infty}^{+\infty} f(x)\overline{g(y+x)}\,dx$$

and the autocorrelation as:

$$(f \star g)(y) = (f * \overline{\tilde{f}})(y) = \int_{-\infty}^{+\infty} f(x)\overline{f(y+x)}\,dx,$$

where for any function f, $\tilde{f}(x)$ is defined as $\tilde{f}(x) = f(-x)$.

We also define the Fourier Transform of a function as:

$$\widehat{f(\xi)} = \mathcal{F}[f(x)] = \int_{-\infty}^{+\infty} f(x)e^{-2\pi i x\xi}\,dx.$$

So, is it true that $\langle f \star f \ , \ g \star g\rangle = \|f \star g\|^2$? The answer is yes.

Lemma 3.2 *Assume that f, g are complex functions in $L^2(\mathbb{R})$. Then,*

$$\langle f \star f \ , \ g \star g\rangle = \|f \star g\|^2,$$

where the inner products and norms are taken w.r.t. $L^2(\mathbb{R})$.

Proof The Fourier Transform is an isometry. So,

$$\begin{aligned} \|f \star g\|^2 &= \langle \widehat{f \star g}, \widehat{f \star g}\rangle \\ &= \langle \hat{f}\hat{\overline{\tilde{g}}} \ , \ \hat{f}\hat{\overline{\tilde{g}}}\rangle \quad \text{(by the Convolution Theorem)} \end{aligned}$$

First, we note that,

$$\begin{aligned} \widehat{\overline{f}(\xi)} &= \langle \overline{f}(x) \ , \ e^{2\pi i x\xi}\rangle \\ &= \langle e^{-2\pi i x\xi} \ , \ f(x)\rangle \\ &= \overline{\langle f(x) \ , \ e^{-2\pi i x\xi}\rangle} \\ &= \overline{\int_{-\infty}^{+\infty} f(x)e^{2\pi i x\xi}\,d\mu(x)} \\ &= \overline{\int_{-\infty}^{+\infty} f(-y)e^{2\pi i(-y)\xi}\,d\mu(y)} \quad \text{(by changing variables } x = -y\text{)} \\ &= \overline{\langle \tilde{f}(y), e^{2\pi i y\xi}\rangle} \\ &= \overline{\widehat{\tilde{f}(\xi)}} \end{aligned}$$

Hence, $\widehat{\overline{\tilde{f}}(\xi)} = \overline{\widehat{f(\xi)}}$.

$$\begin{aligned}
\Longrightarrow \quad \|f \star g\|^2 &= \int_{-\infty}^{+\infty} \widehat{f(\xi)}\,\overline{\widehat{f(\xi)}}\,\overline{\widehat{\tilde{g}(\xi)}\,\overline{\widehat{\tilde{g}(\xi)}}}\, d\mu(\xi) \\
&= \int_{-\infty}^{+\infty} \widehat{f(\xi)}\,\overline{\widehat{f(\xi)}}\,\widehat{g(\xi)}\,\overline{\widehat{g(\xi)}}\, d\mu(\xi) \\
&= \langle \hat{f}\overline{\hat{f}}\ ,\ \hat{g}\overline{\hat{g}} \rangle \\
&= \langle \hat{f}\overline{\hat{\tilde{f}}}\ ,\ \hat{g}\hat{\overline{\tilde{g}}} \rangle \\
&= \langle \widehat{f * \overline{\tilde{f}}}\ ,\ \widehat{g * \overline{\tilde{g}}} \rangle \\
&= \langle f \star f\ ,\ g \star g \rangle \quad \text{(since the F. T. is an isometry).} \qquad \blacksquare
\end{aligned}$$

Furthermore, assume that they

Now suppose instead of a function in $L^2(\mathbb{R})$, we have a function in $L^2([0,1))$. Can we prove a comparable result? The answer is yes. All of the same arguments apply as in the case of $L^2(\mathbb{R})$. The only thing we have to modify is that we note that the map $f \mapsto \widehat{f}$ (where $\widehat{f}$ is the Fourier expansion of f) is an isometric isomorphism between $L^2([0,1))$ and $l^2(\mathbb{Z})$ by the Riesz-Fischer Theorem. Then, we only require that the Fourier series of f and g converge uniformly so that we can interchange the infinite sum and the integral, and all of the previous arguments apply.

Continuing in extending our results from the previous section to spaces of non-discrete functions, such as L^2, we now ask if we can establish a bound similar to the Sarwate one above. Define the following two numbers $\tilde{A}$ and $\tilde{\Gamma}$:

$$\begin{aligned}
\tilde{A} &= \max\{\|u \star u\|_{\sup},\ u \in X\} \\
\tilde{\Gamma} &= \max\{\|u \star v\|_{\sup},\ u, v \in X,\ u \neq v\}
\end{aligned}$$

The next Theorem gives such a result.

Theorem 3.3 *Consider a family $X \subseteq L^2([0,1))$ of K continuous functions s.t. for all $u \in X$, $|\int_0^1 u(x)\, d\mu(x)| = 1$. Then,*

$$\frac{\tilde{A}^2}{K} + (K-1)\frac{\tilde{\Gamma}^2}{K} \geq 1.$$

Proof

$$\sum_{\substack{u\in X\\ u\neq v}}\sum_{v\in X}\|u\star v\|^2+\sum_{u\in X}\|u\star u\|^2$$

$$\begin{aligned}
&= \sum_{u\in X}\sum_{v\in X}\|u\star v\|^2\\
&= \sum_{u\in X}\sum_{v\in X}\langle u\star u\ ,\ v\star v\rangle\\
&= \langle\sum_{u\in X}u\star u\ ,\ \sum_{v\in X}v\star v\rangle\\
&= \|\sum_{u\in X}u\star u\|^2
\end{aligned}$$

Now, as in Lemma 3.2, we note that,

$$(u\star u)(x)=\sum_{k\in\mathbb{Z}}|\hat{u}(k)|^2e^{2\pi ikx},\quad \text{and}\ \ \hat{u}(0)=\int_0^1 u(x)\,d\mu(x)$$

Hence,

$$\begin{aligned}
\|\sum_{u\in X}u\star u\|^2 &= \sum_{u\in X}\sum_{v\in X}\sum_{k\in\mathbb{Z}}|\hat{u}(k)|^2|\hat{v}(k)|^2\\
&= \sum_{u\in X}\sum_{v\in X}\sum_{k\in\mathbb{Z}\backslash 0}|\hat{u}(k)|^2|\hat{v}(k)|^2+\sum_{u\in X}\sum_{v\in X}|\hat{u}(0)|^2|\hat{v}(0)|^2\\
&= K^2+\sum_{u\in X}\sum_{v\in X}\sum_{k\in\mathbb{Z}\backslash 0}|\hat{u}(k)|^2|\hat{v}(k)|^2.
\end{aligned}$$

The left-hand side is bounded from above by $K\tilde{\mathrm{A}}^2+K(K-1)\tilde{\Gamma}^2$ since

$$|f(x)|\leq\|f\|_{\mathrm{sup}}\implies\int_0^1|f(x)|^2\,d\mu(x)\leq\|f(x)\|^2_{\mathrm{sup}}.$$

On the other hand, the right hand side is bounded from below by K^2 since the second term is always non-negative. Hence,

$$K\tilde{\mathrm{A}}^2+K(K-1)\tilde{\Gamma}^2\geq K^2\implies\frac{\tilde{A}^2}{K}+(K-1)\frac{\tilde{\Gamma}^2}{K}\geq 1.\qquad\blacksquare$$

Remark We can easily make this into a more general result, where instead of continuous functions we use any $L^2([0,1))$ functions and substitute the L^2 norm for the sup norm.

4 Rudin-Shapiro Sequences

An area of coding theory where analytic methods are used extensively is the study of codes generated by Generalized Rudin-Shapiro Systems. In our study of these systems, we used George Benke's 1994 paper of the same name [2].

The classical Rudin-Shapiro polynomials are trigonometric polynomials defined recursively as:

$$\begin{aligned} P_0(x) &= 1, \quad Q_0(x) = 1 \\ P_{n+1}(x) &= P_n(x) + e^{2\pi i 2^n x} Q_n(x) \\ Q_{n+1}(x) &= P_n(x) - e^{2\pi i 2^n x} Q_n(x). \end{aligned}$$

Lemma 4.1 *Let $P_n(x)$ and $Q_n(x)$ be as above. Then, for any $n \geq 0$, we have:*

$$|P_{n+1}(x)|^2 + |Q_{n+1}(x)|^2 = 2(|P_n(x)|^2 + |Q_n(x)|^2).$$

Proof

$$\begin{aligned} |P_{n+2}(x)|^2 + |Q_{n+2}(x)|^2 &= \left| P_{n+1}(x) + e^{2\pi i 2^{n+1} x} Q_{n+1}(x) \right|^2 + \left| P_{n+1}(x) - e^{2\pi i 2^{n+1} x} Q_{n+1}(x) \right|^2 \\ &= 2(|P_{n+1}(x)|^2 + |Q_{n+1}(x)|^2) \\ &+ e^{2\pi i 2^{n+1} x} \overline{P_{n+1}(x)} Q_{n+1}(x) + e^{-2\pi i 2^{n+1} x} \overline{Q_{n+1}(x)} P_{n+1}(x) \\ &- e^{2\pi i 2^{n+1} x} Q_{n+1}(x) \overline{P_{n+1}(x)} - e^{-2\pi i 2^{n+1} x} \overline{Q_{n+1}(x)} P_{n+1}(x) \\ &= 2(|P_{n+1}(x)|^2 + |Q_{n+1}(x)|^2). \quad \blacksquare \end{aligned}$$

Lemma 4.2 *For any $n \geq 0$, we have:*

$$|P_n(x)| \leq \sqrt{2}\sqrt{N}, \quad \text{and} \quad |Q_n(x)| \leq \sqrt{2}\sqrt{N}$$

where $N = 2^n = \|P_n(x)\|_2^2 = \|Q_n(x)\|_2^2$.

Proof

$$\begin{aligned}|P_n(x)|^2+|Q_n(x)|^2 &= 2(|P_{n-1}(x)|^2+|Q_{n-1}(x)|^2) \quad \text{(by 4.1)}\\ &= 2*2^{n-1}(|P_0(x)|^2+|Q_0(x)|^2) \quad \text{(applying 4.1 repeatedly)}\end{aligned}$$

But, $|P_0(x)|^2+|Q_0(x)|^2=2$ Hence,

$$|P_n(x)|^2+|Q_n(x)|^2=2*2^n.$$

This means that $|P_n(x)|\leq\sqrt{2}\sqrt{N}$. The same holds true for $Q_n(x)$. $\blacksquare$

Alternatively, we can write this system in matrix-vector form. Let

$$X_n(x)=\begin{pmatrix}P_n(x)\\Q_n(x)\end{pmatrix} \quad U=\begin{pmatrix}1/\sqrt{2} & 1/\sqrt{2}\\1/\sqrt{2} & -1/\sqrt{2}\end{pmatrix} \quad D_n(x)=\begin{pmatrix}1 & 0\\0 & e^{2\pi i2^nx}\end{pmatrix}$$

Hence, Equations (1), (2), and (3) become

$$X_{n+1}=\sqrt{2}UD_n(x)X_n(x).$$

This motivates the generalization of the construction. We begin to generalize it by letting $\epsilon=\{\epsilon_n\}, n=1,2,\ldots,$ be an arbitrary sequence of 0's and 1's, and letting $F=\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$. Then, we define the sequence $X_{\epsilon,n+1}$ as:

$$X_{\epsilon,n+1}(x)=\sqrt{2}UD_n(x)F^{\epsilon_n}X_{\epsilon,n}(x).$$

So, if we consider all the possible choices for ϵ, at each stage n, we obtain 2^n polynomials with 2^n coefficients. So, we form a matrix, where for each polynomial, there is a row of its coefficients. Hence, the first three matrices of the construction are:

$$\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}, \quad \begin{pmatrix}1 & 1 & 1 & -1\\1 & 1 & -1 & 1\\1 & -1 & 1 & 1\\1 & -1 & -1 & -1\end{pmatrix},$$

$$\text{and} \quad \begin{pmatrix}1 & 1 & 1 & -1 & 1 & 1 & -1 & 1\\1 & 1 & 1 & -1 & -1 & -1 & 1 & -1\\1 & 1 & -1 & 1 & 1 & 1 & 1 & -1\\1 & 1 & -1 & 1 & -1 & -1 & -1 & 1\\1 & -1 & 1 & 1 & 1 & -1 & -1 & -1\\1 & -1 & 1 & 1 & -1 & 1 & 1 & 1\\1 & -1 & -1 & -1 & 1 & -1 & 1 & 1\\1 & -1 & -1 & -1 & -1 & 1 & -1 & -1\end{pmatrix}, \quad \text{respectively.}$$

It can be clearly seen that the rows are orthogonal. The first two rows are the N^{th} classical Rudin-Shapiro coefficients. We shall call this construction the "append" rule. It is so called since at each stage of the iteration, new higher-order terms are added to the end of the polynomial. A related, but different, construction is given by:

$$X_{n+1}(x) = \sqrt{2}UT(x)X_n(2x).$$

where

$$T(x) = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi ix} \end{pmatrix}.$$

This is called the interlace rule, since new terms are not added to the end, but rather "interlaced" in between the previous ones. As with the "append" construction, we can also consider the entire set of coefficient blocks generated by all possible ϵ. As in, for each ϵ,

$$X_{\epsilon,n+1}(x) = \sqrt{2}UT(x)F^{\epsilon_n}X_{\epsilon,n}(2x).$$

Now, we can generalize these constructions to arbitrary $p \times p$ matrices. Notice that for the "append" construction, for $n = 1$, the generating matrix was $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Now, we can have the system of polynomials be generated by *any* $p \times p$ matrix, where p is prime.

So, how do we get at this generalization? Note that in the classical Rudin-Shapiro Append rule, given the original matrix $\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$, and two consecutive rows R_i, R_j, we form four new rows for the next iteration:

$$(a_{00}R_i \ a_{01}R_j)\,, \ (a_{10}R_i \ a_{11}R_j)\,,$$

$$(a_{00}R_j \ a_{01}R_i)\,, \text{ and } (a_{10}R_j \ a_{11}R_i)\,.$$

Note how the rows of the previous matrix are cyclically permuted in the construction, and the entries of the original matrix appear as coefficients in the new one. Thus, generalizing this construction to the $p \times p$ case, we see that expressing the row and column indeces in a base-p representation vector is most convenient. Hence, letting $\vec{\omega}, \vec{\nu} \in \mathbb{Z}_p^n$ and $\vec{p} = \{1, p, \ldots, p^{n-1}\}$, the generalized Append and Interlace polynomials ($A_{n,\nu}(x)$ and $I_{n,\nu}(x)$, respectively) are given by:

$$\begin{aligned} A_{n,\nu}(x) &= \sum_{\omega \in \mathbb{Z}_p^n} a_{\nu_0, \omega_{n-1}} \left(\prod_{k=1}^{n-1} a_{\nu_{n-k}+\omega_k, \omega_{k-1}} \right) e^{2\pi i <\vec{p}, \vec{\omega}> x} \\ I_{n,\nu}(x) &= \sum_{\omega \in \mathbb{Z}_p^n} a_{\nu_0, \omega_0} \left(\prod_{k=1}^{n-1} a_{\nu_k+\omega_{k-1}, \omega_k} \right) e^{2\pi i <\vec{p}, \vec{\omega}> x}, \end{aligned}$$

where all subscript addition is computed modulo p.

These generalized Rudin-Shapiro systems have interesting applications to coding theory. One could construct a code using the coefficients of the trigonometric polynomial. How good are these codes, especially in terms of the Sarwate bound proven earlier? First, we change notation slightly and say that $\vec{\nu} \in \mathbb{Z}_p^{p^n}$ is now a code given by the coefficients of the polynomial $A_{n,\vec{\nu}}(x)$.

Lemma 4.3 *Let $n \geq 1$ and $p \geq 2$. Let $\overline{A(n)} = \frac{A}{p^n}$, $\overline{\Gamma(n)} = \frac{\Gamma}{p^n}$ at the n^{th} stage of the process. Also, say that $A = \sqrt{\beta} U$ for some unitary matrix U. Then, for each n,*

$$\overline{A(n)} \leq (\beta/p)^n \text{ and } \overline{\Gamma(n)} \leq (\beta/p)^n.$$

Proof For each $l \geq 1, \alpha(u)(l) \leq \alpha(u)(0)$ since the autocorrelation function peaks at zero-shift. Now note that for each code $\vec{\nu}$, $\alpha(\vec{\nu})(0) = \int_0^1 |A_{n,\vec{\nu}}(x)|^2 \, dx = \beta^n$ by Theorem 5 in [2]. Hence,

$$\overline{A(n)} = \frac{A}{p^n} \leq \frac{\max\{\alpha(\vec{\nu})(0), \vec{\nu} \in \mathbb{Z}_p^{p^n}\}}{p^n} = \left(\frac{\beta}{p}\right)^n$$

Now, for Γ, observe that if we represent our sequences, $\vec{\nu}, \vec{\nu}'$ as vectors, we can write

$$\gamma(\vec{\nu}, \vec{\nu}')(l) = \langle \vec{\nu}, S_l \vec{\nu}' \rangle,$$

where S_l is the linear transformation that shifts a vector cyclically by l places. Since $S_l \in \mathsf{Sym}(p^n)$, it is an isometry of $\mathbb{R}^{p^n}$. Hence,

$$|\gamma(\vec{\nu}, \vec{\nu}')(l)| \leq \|\vec{\nu}\| \, \|S_l \vec{\nu}'\| = \|\vec{\nu}\| \, \|\vec{\nu}'\| = \|A_{n,\vec{\nu}}\|_2 \, \|A_{n,\vec{\nu}'}\|_2$$

But, by Theorem 5 in [2],

$$\|A_{n,\vec{\nu}}\|_2 \, \|A_{n,\vec{\nu}'}\|_2 = \beta^n.$$

Hence, $\overline{\Gamma(n)} = \frac{\Gamma}{p^n} \leq \left(\frac{\beta}{p}\right)^n$. ▮

Lemma 4.4 *Let $A = \sqrt{\beta}U$, for some unitary matrix U and constant β. Let $\vec{\nu}$ be the code given by the coefficients of the Append polynomial, $A_{n,\vec{\nu}}(x)$. Then, the Discrete Fourier Transform of $\vec{\nu}$ is given by:*

$$\widehat{\vec{\nu}} = \{\frac{1}{p^n}A_{n,\vec{\nu}}(0), \frac{1}{p^n}A_{n,\vec{\nu}}(\frac{-1}{p^n}), \ldots, \frac{1}{p^n}A_{n,\vec{\nu}}(\frac{1-p^n}{p^n})\}$$

.

Proof By the definition of the DFT, if $\vec{\nu} = \{\nu_0, \nu_1, \ldots, \nu_{p^n-1}\}$, then

$$\widehat{\vec{\nu}} = \{\chi_0, \chi_1, \ldots, \chi_{p^n-1}\},$$

where for each m,

$$\chi_m = \frac{1}{p^n} \sum_{k=0}^{p^n-1} \nu_k e^{\frac{-2\pi i k m}{p^n}}.$$

But, note that for each m this sum is just the Append polynomial evaluated at $x = -m/p^n$ since the coefficients ν_k are just the coefficients of $A_{n,\vec{\nu}}(x)$ taken in the same order. Hence,

$$\widehat{\vec{\nu}} = \{\frac{1}{p^n}A_{n,\vec{\nu}}(0), \frac{1}{p^n}A_{n,\vec{\nu}}(\frac{-1}{p^n}), \ldots, \frac{1}{p^n}A_{n,\vec{\nu}}(\frac{1-p^n}{p^n})\}. \quad ▮$$

Lemma 4.5 *Let $\vec{\nu}$ be as above. Then, for each $m = 0, 1, \ldots, p^n - 1$,*

$$|\chi_m| \leq \sqrt{p}\left(\frac{\sqrt{\beta}}{p}\right)^n.$$

Proof By Corollary 4 in [2], for all x, $|A_{n,\vec{\nu}}(x)| \leq \sqrt{p}\left(\sqrt{\beta}\right)^n$. Substituting into the above, we see that for all m,

$$|\chi_m| = \frac{1}{p^n}|A_{n,\vec{\nu}}(\frac{-m}{p^n})| \leq \frac{1}{p^n}\sqrt{p}\left(\sqrt{\beta}\right)^n = \sqrt{p}\left(\frac{\sqrt{\beta}}{p}\right)^n \quad ▮$$

Theorem 4.6 *Say that f is a function in $L^2((0,1])$, such that for all k, $\exists C > 0, a > 1$ such that*

$$|\hat{f}(k)| \leq \frac{C}{a^n},$$

where $\hat{f}(k)$ is the k-th Fourier coefficient. Furthermore, assume that the Fourier series has no more than p^n terms, where p is some prime. Then, $\|f \star f\|_1 \to 0$ as $n \to \infty$.

Proof Say the Fourier series of f has p^n terms. $f \star f = \sum_{k=1}^{p^n} |\hat{f}(k)|^2 e^{2\pi ikx}$, as before. Then, we have that

$$\begin{aligned} f \star f &\leq \sup_{k \leq p^n} |\hat{f}(k)|^2 \sum_{k=1}^{p^n} e^{2\pi ikx} \\ &\leq \frac{C}{a^n} D_{p^n}(x), \end{aligned}$$

where $D_{p^n}(x)$ is the Dirichlet kernel. From standard Fourier Analysis, we know that $\|D_{p^n}(x)\|_1 = \frac{4}{\pi^2} \log p^n + O(1)$ (consult [4] for a complete proof). Hence,

$$\begin{aligned} \|f \star f\|_1 &\leq \frac{C}{a^n}(n \log p + O(1)) \\ &\to 0 + 0 = 0 \end{aligned}$$

as $n \to \infty$. ▮

The above theorem has important consequences for us. Note that for any code $\vec{\nu}$ that satisfies the hypotheses of 4.4, we can see that for each k, the k-th Fourier coefficient of the periodic autocorrelation function $\alpha(\vec{\nu})$ is given by $|\chi_k|^2$ where χ_k is the k-th Fourier coefficient of our code. Now, taking the Inverse DFT of the DFT of the autocorrelation function, we can recover the autocorrelation function itself. But, notice that we can use an argument similar to the one in the preceding theorem to get a bound on the IDFT. Hence, we see that with binary codes given by the classical RS construction as $n \to \infty$, $\alpha(\nu)(l) \to 0$ for all $l \leq 2^n$.

References

[1] P. E. Barbano. Bernoulli Shifts and Communication Codes. *Acta. Math.*, 158:213–313, 1987. Seminare Maurey-Schwartz (1975-1976).

[2] G. Benke. Generalized Rudin-Shapiro systems. *J. of Fourier Analysis and its Applications*, 1:87–101, 1994.

[3] R. Coifman. Noiselets. *Proc. Amer. Math. Soc.*, 49:267–268, 1975.

[4] J. Duoandikoetxea. *Fourier Analysis.* American Mathematical Society, Providence, RI, 2000.

[5] S. W. Golomb. *Shift Register Sequences.* Holden-Day, Inc., San Francisco, 1967.

[6] D. V. Sarwate. Bounds on crosscorrelation and autocorrelation of sequences. *IEEE Trans. Inform. Theory*, 25(6):720–724, 1979.